EXHIBIT 8

The New York Times https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html

Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency

By Nathaniel Popper

Aug. 21, 2017

Hackers have discovered that one of the most central elements of online security — the mobile phone number — is also one of the easiest to steal.

In a growing number of online attacks, hackers have been calling up Verizon, T-Mobile U.S., Sprint and AT&T and asking them to transfer control of a victim's phone number to a device under the control of the hackers.

Once they get control of the phone number, they can reset the passwords on every account that uses the phone number as a security backup — as services like Google, Twitter and Facebook suggest.

"My iPad restarted, my phone restarted and my computer restarted, and that's when I got the cold sweat and was like, 'O.K., this is really serious,'" said Chris Burniske, a virtual currency investor who lost control of his phone number late last year.

A wide array of people have complained about being successfully targeted by this sort of attack, including a Black Lives Matter activist and the chief technologist of the Federal Trade Commission. The commission's own data shows that the number of so-called phone hijackings has been rising. In January 2013, there were 1,038 such incidents reported; by January 2016, that number had increased to 2,658.

But a particularly concentrated wave of attacks has hit those with the most obviously valuable online accounts: virtual currency fanatics like Mr. Burniske.

Within minutes of getting control of Mr. Burniske's phone, his attackers had changed the password on his virtual currency wallet and drained the contents — some $150,000 at today's values.

Most victims of these attacks in the virtual currency community have not wanted to acknowledge it publicly for fear of provoking their adversaries. But in interviews, dozens of prominent people in the industry acknowledged that they had been victimized in recent months.

"Everybody I know in the cryptocurrency space has gotten their phone number stolen," said Joby Weeks, a Bitcoin entrepreneur.

Mr. Weeks lost his phone number and about a million dollars' worth of virtual currency late last year, despite having asked his mobile phone provider for additional security after his wife and parents lost control of their phone numbers.

The attackers appear to be focusing on anyone who talks on social media about owning virtual currencies or anyone who is known to invest in virtual currency companies, such as venture capitalists. And virtual currency transactions are designed to be irreversible.

Accounts with banks and brokerage firms and the like are not as vulnerable to these attacks because these institutions can usually reverse unintended or malicious transactions if they are caught within a few days.

But the attacks are exposing a vulnerability that could be exploited against almost anyone with valuable emails or other digital files — including politicians, activists and journalists.

Last year, hackers took over the Twitter account of DeRay Mckesson, a leader of the Black Lives Matters movement, by first getting his phone number.

In a number of cases involving digital money aficionados, the attackers have held email files for ransom — threatening to release naked pictures in one case, and details of a victim's sexual fetishes in another.

The vulnerability of even sophisticated programmers and security experts to these attacks sets an unsettling precedent for when the assailants go after less technologically savvy victims. Security experts worry that these types of attacks will become more widespread if mobile phone operators do not make significant changes to their security procedures.

"It's really highlighting the insecurity of using any kind of telephone-based security," said Michael Perklin, the chief information security officer at the virtual currency exchange ShapeShift, which has seen many of its employees and customers attacked.

Mobile phone carriers have said they are taking steps to head off the attacks by making it possible to add more complex personal identification numbers, or PINs, to accounts, among other steps.

Business & Economy

Latest Updates ›

Updated 6 hours ago

- A low-carbon economy is cheaper than the costs of climate change, a report says.
- Today in On Tech: These apps deliver food and misery.
- Wall Street rebounds from a four-day slump as the Fed signals its next move.

But these measures have not been enough to stop the spread and success of the culprits.

After a first wave of phone porting attacks on the virtual currency community last winter, which was reported by Forbes, their frequency appears to have ticked up, Mr. Perklin and other security experts said.

In several recent cases, the hackers have commandeered phone numbers even when the victims knew they were under attack and alerted their cellphone provider.

Joby Weeks at a park near his parents' home in Arvada, Colo. Mr. Weeks lost his phone number and about a million dollars' worth of virtual currency last year. Matthew Staver for The New York Times

Adam Pokornicky, a managing partner at Cryptochain Capital, asked Verizon to put extra security measures on his account after he learned that an attacker had called in 13 times trying to move his number to a new phone.

But just a day later, he said, the attacker persuaded a different Verizon agent to change Mr. Pokornicky's number without requiring the new PIN.

A spokesman for Verizon, Richard Young, said that the company could not comment on specific cases, but that phone porting was not common.

"While we work diligently to ensure customer accounts remain secure, on occasion there are instances where automated processes or human performance falls short," he said. "We strive to correct these issues quickly and look for additional ways to improve security."

Mr. Perklin, who worked at a Canadian mobile phone operator before joining ShapeShift, said most phone companies would write down any additional security requests in the notes of a customer account.

But agents can generally act on their own, he said, regardless of what is in the notes, and can easily miss what is in the notes.

The vulnerability of phone numbers is the unintended consequence of a broad push in the security industry to institute a practice, known as two-factor authentication, that is supposed to help make accounts more secure.

Many email providers and financial firms require customers to tie their online accounts to phone numbers, to verify their identity. But this system also generally allows someone with the phone number to reset the passwords on these accounts without knowing the original passwords. A hacker just hits “forgot password?” and has a new code sent to the commandeered phone.

Mr. Pokornicky was online at the time his phone number was taken, and he watched as his assailants seized all his major online accounts within a few minutes.

“It felt like they were one step ahead of me the whole time,” he said.

The speed with which the attackers move has convinced people who are investigating the hacks that the attacks are generally run by groups of hackers working together.

Danny Yang, the founder of the virtual currency security firm BlockSeer, said he had traced several attacks to internet addresses in the Philippines, though other attacks have been tracked to computers in Turkey and the United States.

Mr. Perklin and other people who have investigated recent hacks said the assailants generally succeeded by delivering sob stories about an emergency that required the phone number to be moved to a new device — and by trying multiple times until a gullible agent was found.

“These guys will sit and call 600 times before they get through and get an agent on the line that’s an idiot,” Mr. Weeks said.

Coinbase, one of the most widely used Bitcoin wallets, has encouraged customers to disconnect their mobile phones from their Coinbase accounts.

But some customers who have lost money have said the companies need to take more steps by doing things like delaying transfers from accounts on which the password was recently changed.

“Coinbase looks like a bank, stores millions of dollars like a bank, but you don’t realize how weak its default protections are until you are robbed of thousands of dollars in minutes,” said Cody Brown, a virtual reality developer who was hacked in May.

Mr. Brown wrote a widely circulated post about his experience, in which he lost around $8,000 worth of virtual currency from his Coinbase account, all as he sat online and watched, getting no response from the customer service at either Coinbase or Verizon.

A spokesman for Coinbase said the company “has invested significant resources to build internal tools to help protect our customers against hackers and account takeovers, including compromise through phone porting.”

The irreversibility of Bitcoin transactions has often been lauded as one of the most important qualities of virtual currency because it makes it harder for banks and governments to intervene in transactions.

But Mr. Pokornicky said the virtual currency industry needed to alert new users to the added risk that comes with the new features of the technology.

“It’s powerful to be able to control your money and move things without any permission,” he said. “But that privilege requires a clear understanding of the downside.”

A version of this article appears in print on , Section A, Page 1 of the New York edition with the headline: Hackers Hijack Phone Numbers To Grab Wallets

- Most people shouldn't pay for identity theft protection. Wirecutter, a New York Times-owned recommendation site, found that these types of services are more about monitoring or addressing identity theft, not preventing it.
- Recovering from the effects of identity theft can be incredibly messy and time-consuming. Here are steps to prevent it and what to do if it happens.